Point of View

Evolve Together

Integrated Supply Chains Extend Security Compliance Requirements

Cesar Salazar

Smaller enterprises bear the burden in today's environment.

VISIT **USCLARO.COM**

Claro Enterprise Solutions

Summary

The growing integration of supply chains is leaving small and medium-sized businesses increasingly vulnerable to compliance risk traditionally borne by larger organizations. As government and industry security requirements extend farther downstream, smaller businesses must take steps to secure data, transactions and infrastructure. Absent these measures, they risk losing partners and clients. Because smaller companies often lack the budget, skills and resources to tackle increasingly complex security challenges, they need a managed security services provider to deliver a cost-effective security solution that mitigates risk and meets industry and regulatory standards.

> **"SMALLER BUSINESSES MUST TAKE STEPS TO SECURE DATA, TRANSACTIONS & INFRASTRUCTURE."**

Adherence to Protocols

In the current context, "compliance" means that IT infrastructure processes and protocols follow existing local and international industry standards, as well as address any local requirements for protecting data. By adhering to these protocols, companies minimize the risk of a security breach and the concomitant economic impact.

The data being protected, meanwhile, relates directly to the products and services provided to end customers, and can include customer records, branch addresses, services provided, committed terms, amounts to invoice, etc. Compromising these information assets can subject a company to fines, loss of customers, damage to reputation and, potentially, failure.

As such, IT security compliance is essential to any company, regardless of size. For smaller organizations, however, maintaining the necessary tools and skills in-house can be a resource-draining proposition. Evolving supply chain relationships pose an additional burden. Large corporations increasingly require smaller suppliers to include security compliance in standard contractual commitments. These obligations put intense pressure on smaller firms to address non-tangible requirements that are not part of their core business or competency. Nevertheless, meeting these requirements is essential to maintaining critical business relationships.

> **"COMPANIES MINIMIZE THE RISK OF A SECURITY BREACH."**

Stringent Requirements

Contractual security compliance requirements are becoming more stringent every day. Businesses are recognizing that security incidents often originate with sub-contractors deep within the supply chain. In many cases, suppliers are sub-contracting to myriad additional firms, often without the original customer's knowledge.

In response to this exposure and lack of transparency, large organizations are evaluating the entire supply chain to demonstrate due diligence to customers and market analysts. As a result, smaller suppliers increasingly face questions related to their security compliance posture and growing pressure to incorporate security requirements into contracts as a cost of doing business. From a different perspective, large businesses seek to push the legal burden of compliance down to smaller suppliers.

Developing a security posture that larger partners will find acceptable requires a deep level of technical knowledge, a wide range of specific skill sets and significant cost. An in-house IT team's responsibilities would include patching the computer's operating system, backing up information and connecting securely to the Internet using a VPN. In addition, the team would need to provide ongoing training to maintain awareness of continually evolving social engineering and phishing threats.

Given the rapid and ongoing evolution of security risks, together with the growing complexity of IT environments, smaller organizations can be hard-pressed to maintain an adequate security posture, specifically in the context of supply chain requirements. The demands of managing budget, deciding on new investments, training employees and filling security talent gaps can be overwhelming.

Key Capabilities

Faced with these challenges, many smaller enterprises are turning to third-party managed security service providers. Key capabilities businesses should look for when assessing their options include the following:

- **Experience:** Qualified professionals who can define, implement and execute a security framework are imperative. Because a security strategy must address multiple variables, framework definition requires multiple skills and a wide range of knowledge. Implementation and execution phases require additional skills related to certifications, training and practice. Capabilities must include not only prevention of security incidents, but detection and remediation of successfully attacked systems.

- **Customized Solutions:** Providers should offer flexibility and the ability to define and implement a security solution aligned to a business' specific requirements. Since security is not a one-size-fits-all proposition, businesses require a consultative approach to define needs and determine an appropriate architecture and roadmap.

- **Financial Support:** Strong financial backing and recognition in multiple markets are important factors to consider, as they enable the investment needed to keep pace with constantly evolving technology and risk landscapes.

- **Technology:** Essential technology capabilities include integration, operations and the delivery of actionable threat intelligence between all the tools and devices comprising the solution. Specifically, the ability to identify and cross-reference attack indicators to enable insight into business/vendor/employee touch points and support rapid response is essential.

Questions to Ask

Specific questions to ask potential security providers include the following:

- Do you have the ability to execute and operate a security framework 24x7x365?
- Are you committed to a specific vendor/architecture, or do you define a solution based on organizational and industry requirements?
- Is your solution based on a Capex or Opex model?
- Will you provide the entire solution or are you open to a hybrid environment that deploys in-house skills?
- Beyond a security compliance solution, do you offer managed security services?
- Do you have a 24x7x365 Security Operations Center (SOC)?
- Do you offer vertical solutions that integrate the network up to server and desktop applications?
- Do you offer setup and management of firewalls, routers, intrusion detection and prevention systems, wireless access control, network ports, account control, system hardening, etc. as they relate to network security?
- How does your team stay up to date on evolving threats and vulnerabilities?

Conclusion

In today's environment, cyber attacks can be generated from any number of touch points between a business and its customers, vendors and employees. An effective security and compliance strategy must address industry- and organization-specific compliance requirements related to architecture, processes and tools. In response to continually evolving business conditions, compliance requirements and security threats, moreover, the strategy must dynamically adjust.

About the Author

Cesar Salazar is Vice President of Engineering & Operations at Claro Enterprise Solutions. In this role, he develops and implements the strategic vision for the Operations organization, leads key architectural decisions and oversees internal security operations, large-scale projects and service contracts. He is also responsible for roadmap planning, release management, integrated design, operations solutioning and delivery integration.